

AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

5

Abstract of the Disclosure

A public key authorization infrastructure includes a client program accessible by a user and an application program. A certificate authority issues a long-term certificate that binds a public key of the user to long-term identification information related to the user. A directory stores the issued long-term certificate and short-term authorization information related to the user. A credentials server issues a short-term certificate to the client. The short-term certificate binds the public key to the long-term identification information and to the short-term authorization information. The client presents the short-term certificate to the application program for authorization and demonstrates that the user has knowledge of a private key corresponding to the public key in the short-term certificate. The short-term certificate includes an expiration date, and is not subject to revocation.

"Express Mail" mailing label number: EL384249172US

Date of Deposit: 1-14-00

I hereby certify that this paper of fee is being deposited with the United States Postal Service "Express Mail Post Office to Addresses" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents,

Washington, D.C. 20231

Printed Name Christine M. Welter
Signature Christine M. Welter